. type a plus sign (+) inside this box	+	Γ.`	٦
--	---	-----	---

type a plus sign (+) inside this box PTO/SB/08A (08-00)

Patent and Trademark C...CO: U.S. DEPARTMENT OF COMMERCE

Approved :- through 10/31/2002. OMB 0651-0031

Patent and Trademark C...CO: U.S. DEPARTMENT OF COMMERCE

Index the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Attorney Docket Number

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE TATEMENT BY APPLICANT

(use as many sheets as necessary)

of

Complete if Known **Application Number** 09/900,959 Filing Date July 10, 2001 **First Named Inventor** LAMBERT, Robert Group Art Unit Not Yet Assigned **Examiner Name** Not Yet Assigned

06944.038

ME CO				U.S. PATENT DOC	UMENTS	
Examine Initials*	,	t Number .	ument nd Code ² known)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
JL		5 675 645	A	Schwartz et al.	10-07-1997	
		4 519 036	A	Green, lan M.	05-21-1985	· · · · · · · · · · · · · · · · · · ·
		5 202 995	A	O'Brien, John K.P.	04-13-1993	RECEIVED
		5 511 198	A	Hotta, Kohlchiro	04-23-1996	
		5 524 222	A	Hervin	06-04-96	NOV 1 9 2001
		5,650,948		Gafter	07-22-97	
·			+-			Technology Center 210
			+-			
						· · · · · · · · · · · · · · · · · · ·
 		<u>.</u>	+		- 	
 			+			•
						·

				FOR	EIGN PATENT DOCUMEN	TS		
Examiner initials	Cite No.1	Office ³	Foreign Patent Do Number ⁴	cument Kind Code* (If known)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Unes, Where Relevant Passages or Relevant Figures Appear	Tô
ブピ	•	wo	98 52319	Α	Fleit, Lois	11-19-1998		
	•	FR	2 672 402	٨	Gemplus Cord INT	08-07-1992		
	, •	wo	98 00771	A	Northern Telecom Ltd/	01-08-1998		
						-		
			- 			ļ		-
								-
								1

Examiner Signature	J~	2÷	Date Considered	6/27/05

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U. S. Patent and Trademark Office, Washington, DC 20231, DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

^{*}EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Oraw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Unique citation designation number. See attached Kinds of U.S. Patent Documents. 2 Enter Office that issued the document, by the two-latter code (WIPO Standard ST.3). *For Japanese patent documents, the Indication of the year of the reign of the Emperor must precede the serial number of the patent document. *Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

•				or series and response to t		n: use through 10/31/2002 OME BIA Little: U.S. DEPARTMENT OF C on unless it contains a valid OMB con mplete If Known	s Co ((C) (iber.
		or form 1449B/F	•		Application Number	09/900,959	
	INFO	RMATIO	N DISC	CLOSURE	Filing Date	July 10, 2001	
1CTO	L STAT	EMENT	RY AP	PLICANT	First Named Inventor	LAMBERT, Robert	
	188		DI A	LIOAH	Group Art Unit	Not Yet Assigned	
D	2	(use as man)	y sheets as n	necessary)	Examiner Name	Not Yet Assigned	
•	SIN	2	of	2	Attorney Docket Number	06944.038	

K\$/		OTHER PRIOR ART - NON PATENT LITERATURE DOCUMENTS							
Examiner Cite Initials No.									
JC	,	PAUL KOCHER, JOSHUA JAFFE, and BENJAMIN JUN, Introduction to Differential Power Analysis and Related Attacks, http://www.cryptography.com/dpa/technical/index.html, 1998, San Francisco.							
		PAUL KOCHER, Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and other systems, http://www.cryptography.com//timing attack/paper.html, Downloaded November 11, 1998, San Francisco.							
)		JOHN WHARTON, An introduction to the IntelR MCS-s1TM Single-Chip Microcomputer Family, Intel Application Note AP-69, may 1980, USA.							
		RECEIVED							
		NOV 1 9 2001	_						
		Technology Center 2100							
		·							
			·						

Examiner Signature	1 '	Date Considered	8/27/05
			

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U. S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

^{*}EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Unique citation designation number. ² Applicant is to place a check mark here if English language Translation is attached.